TO: Clerk's Office
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

APPLICATION FOR LEAVE
TO FILE DOCUMENT UNDER SEAL

****
IN RE: APPLICATION FOR WARRANT TO OBTAIN PROSPECTIVE CELL PHONE LOCATION DATA

20-MC-1279
Docket Number

****

SUBMITTED BY: Plaintiff____ Defendant____ DOJ ✓
Name: Andrew Wang
Firm Name: USAO-EDNY
Address: 271 Cadman Plaza East
Brooklyn, New York 11201
Phone Number: 718-254-6311
E-Mail Address: Andrew.Wang2@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES____ NO ✓
If yes, state description of document to be entered on docket sheet:

A) If pursuant to a prior Court Order:
Docket Number of Case in Which Entered:_____
Judge/Magistrate Judge:_____
Date Entered:_____

B) If a new application, the statute, regulation, or other legal basis that authorizes filing under seal

Ongoing criminal investigation; risk of flight and evidence destruction

ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE, AND MAY NOT BE UNSEALED UNLESS ORDERED BY THE COURT.

DATED: Brooklyn, NEW YORK
06/05/2020

Steven M. Gold

U.S. MAGISTRATE JUDGE

RECEIVED IN CLERK'S OFFICE 06/05/2020
DATE

MANDATORY CERTIFICATION OF SERVICE:
A.) ___ A copy of this application either has been or will be promptly served upon all parties to this action, **B.)** ___ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation:_____; or **C.)** ✓ This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

06/05/2020
DATE

SIGNATURE

WK:ADW
F. #2019R01108

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF THE CELLULAR TELEPHONE ASSIGNED CALL NUMBER (347) 249-2432	Case No. 20-MC-1279 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Alexander Turczak, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the cellular telephone assigned call number (347) 249-2432 (the "SUBJECT PHONE"), whose service provider is T-Mobile US, Inc. ("T-Mobile"), a wireless telephone service provider with operations at 4 Sylvan Way, Parsippany, New Jersey. The SUBJECT PHONE is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," see 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. See 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. See 18 U.S.C. § 3123(b)(1).

3. I am a Special Agent with the Federal Bureau of Investigation, and have been since September 2017. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been involved in the investigation of numerous cases involving mail fraud, wire fraud and money laundering. I have also received training on the uses and capabilities of cellular telephones in connection with criminal activity.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1341 (mail fraud), 1343 (wire fraud), 1349 (conspiracy to commit mail fraud and wire fraud) and 1956 (money laundering and conspiracy to commit money laundering) (collectively, the "Subject Offenses") have been committed, are being committed, and will be committed by Kenneth Ukhuebor. There is also probable cause to believe that the location information described in Attachment B will constitute evidence of these criminal violations, and will lead to the identification of individuals who are engaged in the commission of the Subject Offenses.

6. The Court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, see 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. Kenneth Ukhuebor is a subject in the government's investigation of an Elder Fraud scheme and an apparently separate Business Email Compromise ("BEC") scheme, both of which appear to have been ongoing since as early as the spring of 2019. Ukhuebor appears to have opened several bank accounts in his own name and the business name Kenbor Incorporated ("Kenbor Inc.") in order to perpetrate such fraudulent schemes by receiving hundreds of thousands of dollars in proceeds of Elder Fraud and BEC scams.

Kenneth Ukhuebor's Relationship with Kenbor Inc.

8. Kenbor Inc. is a business corporation registered in New York State. Based on New York State Division of Corporations records, Kenbor Inc. was first registered in March 2015 and lists an individual named Patience Osagie as the person who should receive any legal process on behalf of the company. As described below, Kenbor Inc. appears to be either the business operating name or the parent company of a clothing store operating as Kenbor Clothing.[1]

9. On the business social networking website LinkedIn, a search for the name "Patience Osagie" yields five results. Four of those results are for users listed as residing in Nigeria or the United Kingdom. One of the results is for a user listed as residing in the New York City area. The Patience Osagie residing in the New York City area describes her work experience as being a boutique owner and fashion designer at Kenbor Inc. since January 2015. Notably, this account displays as a profile picture a heavyset adult male with a distinctive beard

[1] Notably, "Kenbor" appears to be a combination of "Kenneth" and "Ukhuebor."

and wearing sunglasses. As described in more detail below, this individual appears to be Kenneth Ukhuebor.

10. Through my investigation, I have identified two separate accounts on the social networking website Facebook, Inc. ("Facebook") that appear to belong to Kenneth Ukhuebor. The username for one of the accounts is "Kenneth Ukhuebor," and the username for the other account is "Ken Kenbor." Both accounts display profile pictures and other photographs depicting the same heavyset adult male shown in the profile picture for the aforementioned Patience Osagie LinkedIn account.

11. A woman named Precious Ukhuebor appears to be Kenneth Ukhuebor's wife. A Facebook account with the username "Precious Ukhuebor" lists the user as "married." On February 14, 2020, the Precious Ukhuebor Facebook account posted a photo of a woman with the heavyset male believed to be Kenneth Ukhuebor and included a Valentine's Day message. In addition, the same Precious Ukhuebor appears to have an account (username "ukhuebor_precious") on Instagram, a social networking site that allows users to post pictures with captions. Precious Ukhuebor's Instagram page includes numerous photos of Kenneth Ukhuebor with accompanying descriptions that refer to him as her husband.

12. The URL for the Precious Ukhuebor Facebook account is www.facebook.com/patience.osagie.3958.

13. On her Facebook account, Precious Ukhuebor describes her employment as "Kenbor Clothing," using a clickable link that leads to a "Kenbor Clothing" Facebook page. The page describes the business as a "Women's Clothing Store" and includes a post from October 16, 2019 announcing a grand opening. The Kenbor Clothing Facebook page displays the following image as its profile picture:

14. On October 16, 2019, Precious Ukhuebor changed her Facebook profile picture to display the same Kenbor Clothing picture above. Also on October 16, 2019, both the Ken Kenbor and Precious Ukhuebor Facebook users posted links to the Kenbor Clothing Facebook page's grand opening announcement.

15. Records from Facebook reveal that both the Kenbor Clothing and the Ken Kenbor accounts were registered using the same phone number.

16. Based on the foregoing, I believe that Patience Osagie and Precious Ukhuebor are either the same person or close associates of one another. The above information also shows that Kenneth Ukhuebor is married to Precious Ukhuebor and, through his wife, is affiliated with Kenbor Inc.

The Elder Fraud Scheme

17. Elder Fraud schemes often involve fraudsters who target elderly victims by pretending to be the representatives of a foreign national lottery (in which the victim has purportedly won a large sum of money) or a foreign estate (in which the victim has purportedly been named as a beneficiary of the estate and is entitled to a large sum of money). Such schemes

sometimes involve promises by fraudsters that the victim will receive a large payment upon the victim's payment to the fraudsters of purported taxes, fees or other invented charges.

18. Persons involved in laundering the proceeds of fraudulent schemes through financial institution accounts and otherwise may receive and transfer funds from multiple such schemes at the same time.

19. Among other things, we have learned through our investigation that in or about the spring of 2019, an unknown person faxed a letter to an 86-year old victim (the "Victim"), the identity of whom is known to me, in New York. The faxed letter stated that the Victim was entitled to a $26.7 million inheritance following the death of an individual in Spain. The letter directed the Victim to send "taxes" and "fees" related to the inheritance to two Bank of America accounts, one bearing the number XXXXXXXX0762 (the "0762 Account") and the other bearing the number XXXXXXXXX8304 (the "8304 Account"). Bank of America signature cards show that the 0762 Account was opened by and in the name of Kenneth Ukhuebor in March 2013, and that the 8304 Account was opened by Patience Osagie, in April 2015, in the name of Kenbor Inc. In total, the Victim sent more than $200,000 in proceeds to the 0762 Account and the 8304 Account.

The BEC Scheme

20. BEC schemes often involve a computer hacker gaining unauthorized access to a business email account via software, malware or social engineering, blocking or redirecting communications to and/or from the email account, and then using the compromised email account or a separate fraudulent email account (sometimes called a "spoofed" email

account)[2] to communicate with unsuspecting personnel from a victim company and trick them into making an unauthorized wire transfer. The fraudster directs the personnel to transmit company funds to the bank account of a third party (sometimes referred to as a "money mule"), which is often a bank account owned, controlled and/or used by individuals involved in the scheme. The money may then be laundered by transferring it through numerous bank accounts or by quickly withdrawing it as cash, by check or by cashier's check.

21. The Philadelphia Sign Company ("PSC"), a New Jersey-based sign design, manufacturing and installation company that does business throughout the United States, is one of the victims of the BEC scheme we are investigating. In July 2019, PSC reported to the government that unidentified persons had gained access to PSC's corporate email account and proceeded to send unauthorized emails to numerous PSC clients. For example, Allstate Corporation, a PSC client, wired almost $400,000 to TD Bank account number XXXXXX4749 (the "4749 Account") at the direction of a fraudster sending an unauthorized email that purported to be from PSC.

22. A TD Bank signature card shows that Kenneth Ukhuebor opened the 4749 Account in his own name in April 2013. In addition, TD Bank surveillance camera footage shows that between May 14, 2019 and June 26, 2019, the heavyset man identified as Kenneth

---

[2] One way of spoofing an email address is to create an account at a fraudulent domain, where the domain name is altered to appear identical to a real company domain but where it is misspelled by a letter or character. For example, a BEC fraudster might spoof the email address of "John" at "ACME, Inc." (john@acmecompany.com) by creating similar email accounts at a fraudulent domain (e.g., john@acmecornpany.com, replacing the "m" in "company" with the letters "rn," or john@acmecompanies.com). Also, BEC fraudsters sometimes create a fraudulent email account at a legitimate email provider (e.g., john_acmecompany@gmail.com).

Ukhuebor and shown in pictures displayed on (a) the Ken Kenbor Facebook account, (b) the Patience Osagie LinkedIn account, and (c) the Precious Ukhuebor Facebook and Instagram accounts, conducted transactions on the 4749 Account at multiple TD Bank locations.

23. Another victim of the BEC scheme was Meristem Packaging Company LLC ("Meristem"), a packaging company based in Georgia. On or about May 8, 2019, Meristem received two emails from nichole.young@eateryesentials.com, a "spoofed" email account purporting to come from Eatery Essentials, a U.S. company that sells and markets paper and plastic cups and containers. At the direction of the emails sent from the spoofed account, Meristem redirected approximately $72,000 in payments to a TD Bank account number XXXXXX3439 (the "3439 Account"). TD Bank records show that Patience Osagie opened the 3439 Account in January 2019, in the name of Kenbor Inc.

The Subject Phone's Connection to the Elder Fraud & BEC Schemes

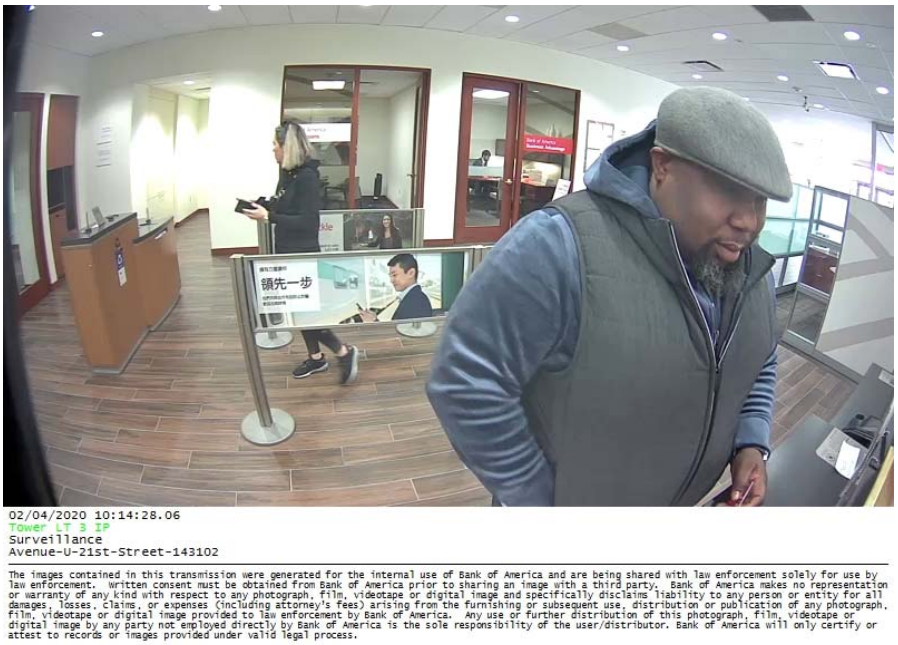
24. Records from Facebook, Inc. reveal that the "Ken Kenbor" Facebook profile is associated with the Yahoo email account kenborpat@yahoo.com.

25. Records from Oath Holdings Inc. (Yahoo's parent company) and T-Mobile reveal that a number of the IP addresses through which the kenborpat@yahoo.com account was repeatedly accessed were associated with the SUBJECT PHONE.

26. Records received from TD Bank, Bank of America, Wells Fargo and JPMorgan Chase show that an individual using the name "Alex Osato" currently maintains accounts with each of those banks and provided the SUBJECT PHONE number when opening the accounts. Each of those accounts has been flagged internally by the respective banks as engaging in suspicious activity. "Alex Osato" opened TD Bank account number XXXXXX8586 (the "8586 Account") using a Nigerian passport that appears to be fraudulent. "Alex Osato"

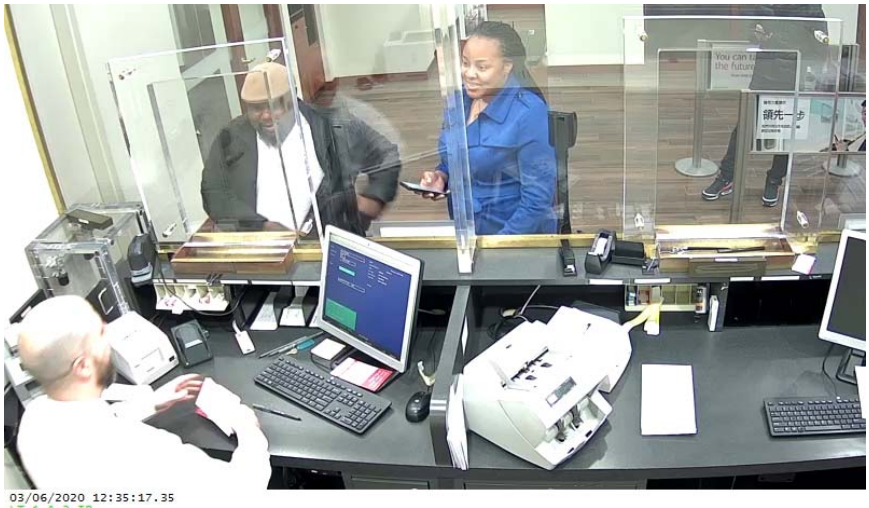
also provided 2811 Avenue U in Brooklyn, New York 11229 as an address when opening the 8586 Account. This is the same address listed for Kenbor Clothing on its Facebook page and several online business listings.

27. "Alex Osato's" account with Bank of America is assigned number XXXXXXXX3717 (the "3717 Account"). Bank of America records show that the man believed to be Kenneth Ukhuebor has been consistently and recently making withdrawals and deposits from the 3717 Account. For example, the following surveillance camera image shows that the heavyset bearded man believed to be Kenneth Ukhuebor was the individual who made a $5,000 cash withdrawal from the 3717 Account on February 4, 2020:

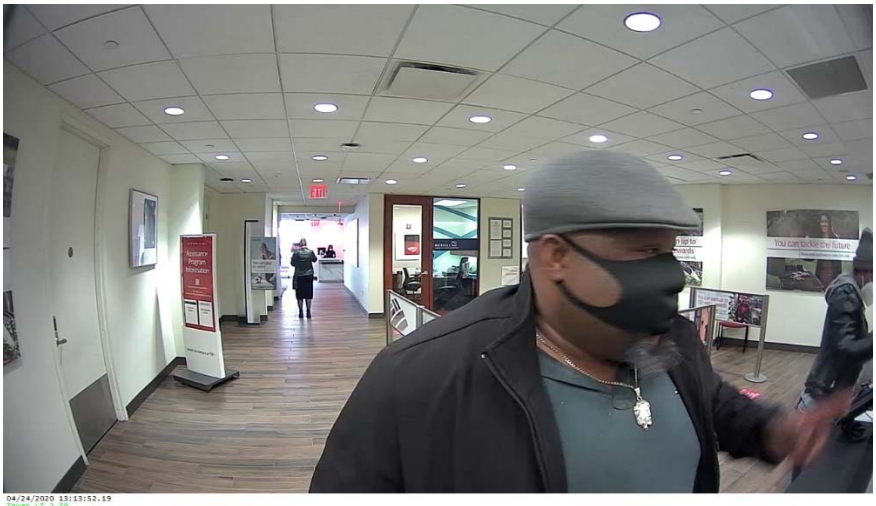


28. The following surveillance camera image shows that Kenneth Ukhuebor withdrew $4,000 in cash from the 3717 Account on March 4, 2020:

29. The following surveillance camera image shows that Kenneth Ukhuebor withdrew $9,000 in cash from the 3717 Account on March 6, 2020:



30. The following surveillance camera image shows that Kenneth Ukhuebor withdrew $9,000 in cash from the 3717 Account on April 24, 2020:



31. The following surveillance camera image shows that Kenneth Ukhuebor deposited $21,545 in cash into the 3717 Account on April 30, 2020:

32. Based on these facts, as well as my training, experience and involvement in this investigation, I believe that prospective location data for the SUBJECT PHONE will provide evidence of Kenneth Ukhuebor's and others' involvement in the Subject Offenses. For example, among other things, location data for the SUBJECT PHONE may reveal the presence of Kenneth Ukhuebor or an accomplice at bank locations to access or manage fraudulent proceeds deposited in the 4749 Account, the 3717 Account or other bank accounts associated with Kenneth Ukhuebor, Precious Ukhuebor, Patience Osagie, Alex Osato, Kenbor Inc. and others.

33. In my training and experience, I have learned that T-Mobile is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including E-911 Phase II data, also known as GPS data or latitude-longitude data and cell-site data, also known as "tower/face information" or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data.

34. Based on my training and experience, I know that T-Mobile can collect E-911 Phase II data about the location of the SUBJECT PHONE, including by initiating a signal to determine the location of the SUBJECT PHONE on T-Mobile's network or with such other reference points as may be reasonably available.

35. Based on my training and experience, I know that T-Mobile can collect cell-site data about the SUBJECT PHONE. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as T-Mobile typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

AUTHORIZATION REQUEST

36. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).

37. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the SUBJECT PHONE would seriously jeopardize the ongoing investigation, as such a

disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. See 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. See 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. See 18 U.S.C. § 3103a(b)(2).

38. I further request that the Court direct T-Mobile to disclose to the government any information described in Attachment B that is within the possession, custody, or control of

T-Mobile. I also request that the Court direct T-Mobile to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference T-Mobile's services, including by initiating a signal to determine the location of the SUBJECT PHONE on T-Mobile's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate T-Mobile for reasonable expenses incurred in furnishing such facilities or assistance.

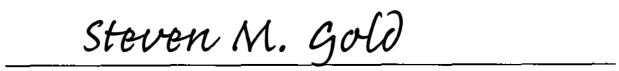
39. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the SUBJECT PHONE outside of daytime hours.

40. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Alexander Turczak
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone on June 5, 2020, 2020



HONORABLE STEVEN M. GOLD
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

1. The cellular telephone assigned call number (347) 249-2432 (the "SUBJECT PHONE"), whose wireless service provider is T-Mobile US, Inc., a company with operations at 4 Sylvan Way, Parsippany, New Jersey (the "Provider").

2. Records and information associated with the SUBJECT PHONE that is within the possession, custody, or control of the Provider, including information about the location of the cellular telephone if it is subsequently assigned a different call number.

ATTACHMENT B

Particular Things to Be Seized

I. Information to Be Disclosed by the Provider

All information about the location of the SUBJECT PHONE described in Attachment A for a period of thirty days, during all times of day and night. "Information about the location of the SUBJECT PHONE" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which "cell towers" (i.e., antenna towers covering specific geographic areas) and "sectors" (i.e., faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Provider, the Provider is required to disclose the Location Information to the government. In addition, the Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Provider's services, including by initiating a signal to determine the location of the SUBJECT PHONE on the Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Provider for reasonable expenses incurred in furnishing such facilities or assistance.

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. See 18 U.S.C. § 3103a(b)(2).

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Sections 1341, 1343, 1349 or 1956 involving Kenneth Ukhuebor.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.